

# Turbulence as a Resource for Quantum Key Distribution in Long Distance Free-Space Links

Giuseppe Vallone,<sup>1</sup> Davide Marangon,<sup>1</sup> Matteo Canale,<sup>1</sup> Ilaria Savorgnan,<sup>1</sup> Davide Bacco,<sup>1</sup> Mauro Barbieri,<sup>2</sup> Simon Calimani,<sup>1</sup> Cesare Barbieri,<sup>2</sup> Nicola Laurenti,<sup>1</sup> and Paolo Villoresi<sup>\*1</sup>

<sup>1</sup>*Department of Information Engineering,*

*University of Padova, via Gradenigo 6/B, 35131 Padova, Italy*

<sup>2</sup>*Department of Physics and Astronomy, University of Padova,*

*vicolo dell'Osservatorio 3, 35122 Padova, Italy*

(ΩDated: April 7, 2014 \*e-mail: paolo.villoresi@dei.unipd.it)

Quantum Key Distribution (QKD) allows to share random keys between two users with unconditional security: the key is usually generated by exchanging a stream of photons. The long-term vision of QKD is represented by a quantum network, implemented by fiber and free-space links involving ground and/or satellites stations. The presence of the atmospheric turbulence represents an obstacle for free-space quantum communications, due to the increase of optical losses. Here we introduce a method to exploit the atmospheric turbulence as a resource for QKD. An Adaptive Real Time Selection (ARTS) technique at the receiver allows to take advantage of the fluctuating transmissivity of the channel, giving rise to an increase of the secure key rate.

## I. INTRODUCTION

The transmission of quantum states to a receiver located far away on the Earth or on some mobile or even orbiting stations is the frontier of Quantum Communications, aiming to extend the networking currently available through fiber to a planetary scale and beyond [1].

The protocols devised for such purposes rely on the transmission and detection of quantum bits - or qubits - that are most conveniently encoded in single light-quanta. In free-space communications, background photons are always present, together with detector non-idealities such as dark counts and dead-time. These effects are detrimental to the quantum protocol accomplishment. In the case of the most common example so far, that is quantum key distribution (QKD), a threshold on the overall quantum bit error rate (QBER), due to experimental imperfections and noise, limits the possibility of exchanging a secure key, because the unconditional secrecy of the key cannot be guaranteed if the QBER exceeds such threshold.

Current demonstrations of QKD have avoided the condition of normal background by operating in dark nights or by using a very strict filtering that imposes a low key rate already on urban scale [2-8]. Due to unavoidable background photons, the QBER will be below the secure threshold only in case of high channel transmission. However, aiming at QKD over long links in realistic conditions including daylight, a breakthrough in the protocol is needed. We devise here a solution that, by exploiting the atmospheric turbulence, allows secret key generation in a part of the link time, even when the average transmission is below the limit of secure communication.

In a link with fluctuating transmission coefficient and a significant attenuation, due to turbulence and to the combination of optical diffraction and scintillation, respectively, it is possible to devise a solution to the high QBER problem on the base of a sound characterization of the channel transmission. A recent study pointed out that the temporal profile of the transmissivity typically has peaks lasting a few milliseconds, distributed in a low transmissivity background [9]. A post-selection technique based on estimating the QBER in short time frames would be ineffective here because the QBER value cannot be reliably estimated in this time scale. Indeed, using current or even realistic transmission rates, the QBER statistics results too limited due to the moderate rate. Moreover, such use of the received qubits further reduces the key rate and has to be avoided.

The CAD1 and CAD2 distillation schemes discussed in [10] represent a generalization of Maurers advantage distillation technique [11]. They collect sequences of correct (possibly non consecutive) sifted bits, and distill one single secure bit out of each sequence. The length of each sequence should be chosen according to a tradeoff. In fact, longer sequences allow to distill keys with higher

channel QBERs, but provide a lower key rate in the case of low QBERs. However, in a turbulent, rapidly time-varying channel, its effectiveness would be limited by the difficulty of choosing the suitable parameters of the distillation strategy according to the varying QBER.

Another generalization of the advantage distillation in [11] is proposed in [12], where parities for many pairs of bits are shared between Alice and Bob along the public channel and those pairs with non matching parities are discarded, while the remaining ones (over which the QBER is lower) are syndrome decoded. However, the above presented distillation methods do not take advantage of the intrinsic QBER variability of the channels, rather they rely on the assumption that the channel maintains its QBER stable for long so that parameters can be optimized.

On the contrary, the technique proposed in [13] relies on detecting transmissivity peaks in the channel by observing variations of the sifted bit rate on a millisecond time scale, and can hence be quite effective in dealing with turbulent channels.

We here propose an adaptive real time selection (ARTS) scheme where transmissivity peaks are instantaneously detected. In fact, an additional resource may be introduced to estimate the link transmissivity in its intrinsic time scale with the use of an auxiliary classical laser beam copropagating with the qubits but conveniently interleaved in time. In this way the link scintillation is monitored in real time and the selection of the time intervals of high channel transmissivity corresponding to a viable QBER for a positive key generation is made available.

In this work we present a demonstration of this protocol in conditions of losses equivalent to long distance and satellite links, and with a range of scintillation corresponding to moderate to severe weather. A useful criterion for the preselection of the low QBER interval is presented that employs a train of intense pulses propagating in the same path as the qubits, with parameters chosen such that its fluctuation in time reproduces that of the quantum communication.

## II. PRELIMINARY ANALYSIS

The link used in our demonstration is the 143 Km free-space channel between La Palma and Tenerife islands shown in figure 1. At the transmitter we generate the quantum bits by strongly attenuated lasers at 850 nm. In the same location we also use a 30 mW<sup>1</sup> classical laser beam (probe) at 808 nm to estimate the link transmissivity. We used two different wavelengths to easily separate, by a dichroic mirror, the two signals at the receiver. The quantum and probe signals are coupled into the same optical path of a customly designed telescope (see figure 1 and Appendix

---

<sup>1</sup> At the transmitter the beam diameter size is of the order of 20cm, guaranteeing class-1M eye-safe beam.

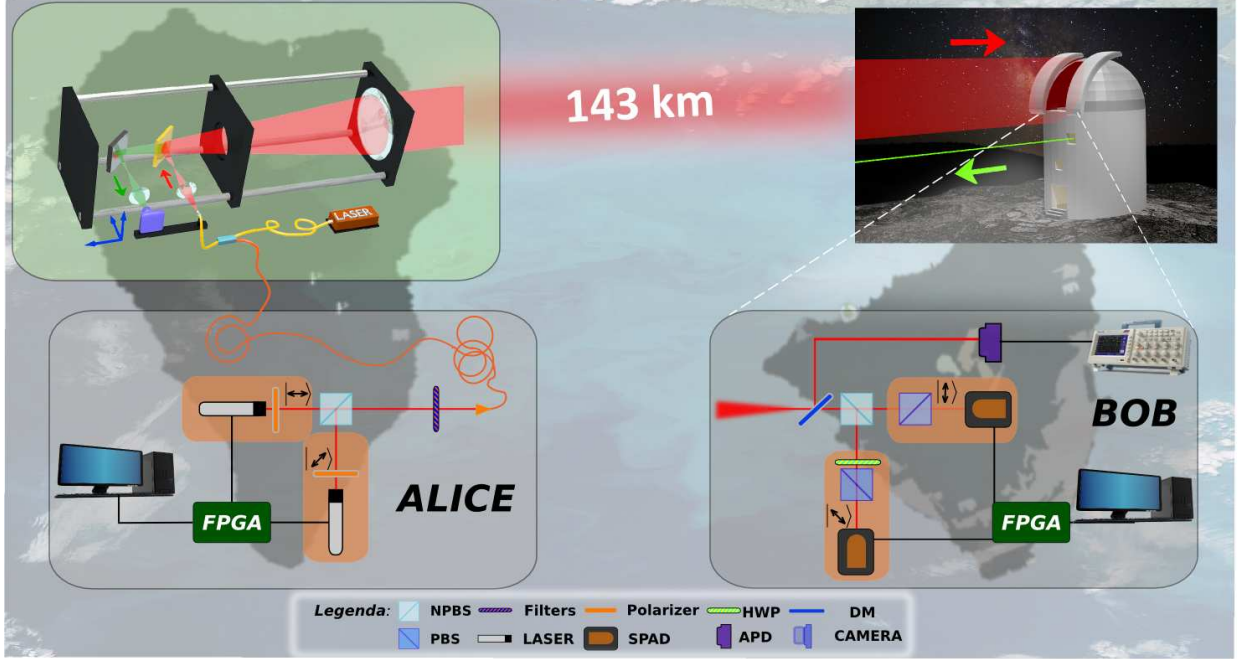


FIG. 1. Experimental setup: Alice, located at JKT observatory in La Palma, sends qubits by using two 850 nm FPGA-controlled attenuated lasers with different polarization. Qubit photons are combined with an atmospheric probe laser (30mW @ 808 nm) and transmitted through a suitably designed telescope. The Alice telescope is also used to collect the beacon laser sent by Bob, located at the Optical Ground Station in Tenerife, and required for tracking the pointing of the transmitter. Bob receives both the signals through the OGS telescope (see Appendix): the probe is monitored by an APD and the qubits are detected with two SPADs. FPGA: Field Programmable Gate Arrays; HWP: half-wave plate; NPBS: non-polarizing beam splitters; PBS, polarizing beam splitter; SPAD, single-photon avalanche photodiode; DM: dichroic mirror.

section).

In order to test the ability of estimating the link transmissivity, we first sent on the same free-space channel, two signals: the classical probe, detected with a fast photodiode at the receiver, and a single strongly attenuated laser. The classical signal featured pulses of  $100 \mu\text{s}$  duration at 1 kHz repetition rate, while the attenuated laser at 850 nm was a continuous beam. At the receiver, the quantum signal was detected by a Single Photon Avalanche Photodiode (SPAD) and acquired in packets with duration of 1 ms.

We would like to test the correspondence between the intensity of the received classical beam and the photons received on the quantum channel. In Figure 2 we show, for 11 s of acquisition time, the photon counts detected in each packet, compared to the voltage registered by the fast photodiode. As it can be seen in the inset, there is a strong correspondence between the two signals.

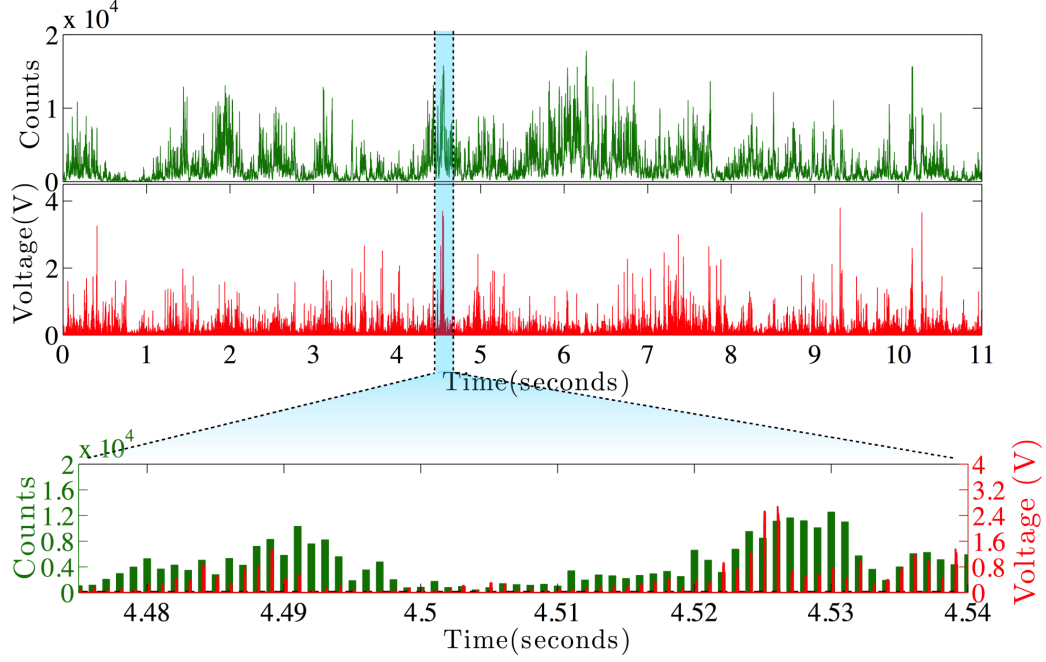


FIG. 2. Comparison between the counts detected by the SPAD (green line) and the voltage measured by the fast photodiode at the receiver (red line). In the inset we show a zoomed detail of the acquisition in order to better appreciate the correlation between the quantum and classical signal.

To demonstrate the correlation we performed the ARTS method, consisting in the following procedure. Given a set of  $L$  packets (each of  $1ms$  length), we let  $V_i$  be the probe signal amplitude and  $S_i$  the number of detected photons in the quantum signal for the  $i$ -th packet, respectively. We set a threshold value  $V_T$  for the probe voltage and post-select only those packets such that  $V_i > V_T$ ; in particular, we denote by  $\mathcal{I}(V_T) = \{i \in [1, L] : V_i > V_T\}$  the indexes of the packets for which the above condition holds and by  $N_P(V_T)$  the corresponding number of packets, that is,  $N_P(V_T) = |\mathcal{I}(V_T)|$ . Furthermore, we define the following quantities:

$$S(V_T) = \sum_{i \in \mathcal{I}(V_T)} S_i, \quad \bar{S}(V_T) = \frac{S(V_T)}{N_P(V_T)} \quad (1)$$

with  $S(V_T)$  representing the total number of detected bits and  $\bar{S}(V_T)$  the mean number of detection per packets after the post-selection performed with threshold  $V_T$ .

The effect of the ARTS procedure can be clearly appreciated in Fig. 3, where  $\bar{S}(V_T)$  (normalized to the mean counts obtained without thresholding) is plotted (green line) as a function of the threshold: a higher threshold value corresponds to a larger mean number of counts per packet. This demonstrates that the probe and quantum signals are strongly correlated and one can significantly

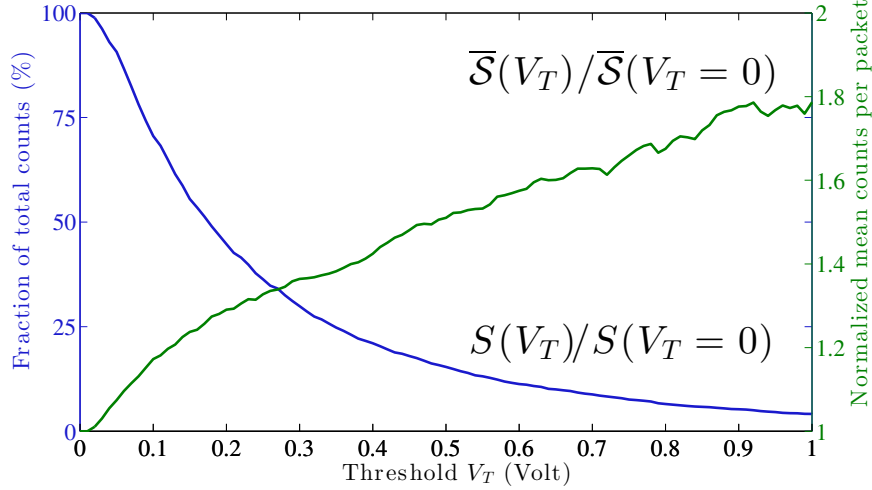


FIG. 3. Mean counts per packet  $\bar{S}(V_T)$  (normalized to the mean counts obtained without thresholding) and fraction of total count  $S(V_T)/S(V_T = 0)$  in function of the probe threshold.

improve the signal-to-noise ratio (SNR) by thresholding<sup>2</sup>. As side effect, we have that the pre-selection also decreases the overall number of detections in the transmission  $S(V_T)$  as can be noticed by considering the ratio  $S(V_T)/S(V_T = 0)$  (blue line).

### III. APPLICATION OF ARTS METHOD TO QKD

We then apply the results previously described to a QKD experiment. In particular, we will show that, increasing the SNR by thresholding gives, in some cases, benefits in terms of the secret key length, even if the total number of sifted bits will decrease. In fact, when the QBER is above 11%, the maximum QBER tolerable for standard QKD, ARTS will reduce the QBER below this limit, allowing secure key generation. We point out that at the receiver the beam has a mean photon number per pulse below 1, namely it is the single photon level. At the transmitter side, due to the 30dB average attenuation of the channel we are not working in the single photon regime (see Appendix).

First, given the number of errors  $E_i$  in the  $i$ -th packet, we define the overall number of errors  $E(V_T)$  and the quantum bit error rate  $Q(V_T)$  in the post-selected packets as

$$E(V_T) = \sum_{i \in \mathcal{I}(V_T)} E_i, \quad Q(V_T) = \frac{E(V_T)}{S(V_T)}. \quad (2)$$

For evaluating the actual impact of the ARTS on the performance of a quantum key distribution system, it is then important to study how the two complementary effects of thresholding: the

<sup>2</sup> Here we define the SNR as the ratio between the overall signal (true signal plus background) and the background

increase of mean detected bits per packet  $\bar{S}(V_T)$  and the decrease of total detections  $S(V_T)$  influence the achievable secret key rate of the system, and the optimal trade-off should be found.

Being the length of the output secret key dependent on the number of available sifted bits and on their bit error rate, as a first step we need to derive an expression for both of these quantities. As demonstrated in [9], the statistics of the transmission of a long free-space channel follows a log-normal distribution. The measured probe voltage at the receiver, being constant the transmitted intensity, follows the same distribution, given by  $p(V; m_V, \sigma^2) = \frac{1}{\sqrt{2\pi}\sigma} \frac{1}{V} e^{-[\ln \frac{V}{m_V} + \frac{1}{2}\sigma^2]^2 / (2\sigma^2)}$ . In the previous expression  $\sigma^2$  is defined as functions of the mean  $m_V$  and of the variance  $v_V$  of the probe intensities distribution, that is,  $\sigma^2 = \ln \left( 1 + \frac{v_V}{m_V^2} \right)$ . As an example, we show in Appendix, the distribution of the measured voltages of the data used in Figure 2, that, according to the theory [9, 14], follows a log-normal distribution.

In the following analysis, we assume that the number of detected photons and the probe intensity have completely correlated log-normal distributions [9]. This trivially implies that both distributions have the same parameter  $\sigma^2$ . By this hypothesis, we can predict the number of packets above threshold  $N_P(V_T)$  and the number of sifted bits surviving the thresholding  $S(V_T)$  in case of null background by  $S(V_T)/S(0) = \int_{V_T}^{+\infty} \frac{V}{m_V} p(V; m_V, \sigma) dV$  and  $N_P(V_T)/N_P(0) = \int_{V_T}^{+\infty} p(V; m_V, \sigma) dV$ . By taking into account the background clicks we get:

$$\begin{aligned} N_P(V_T) &= N_P(0) \frac{1}{2} \left[ 1 - \operatorname{erf} \left( \frac{\ln \frac{V_T}{m_V} + \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}} \right) \right] \\ S(V_T) &= n_b N_P(V_T) + \frac{1}{2} [S(0) - n_b N_P(0)] \left[ 1 - \operatorname{erf} \left( \frac{\ln \frac{V_T}{m_V} - \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}} \right) \right], \end{aligned} \quad (3)$$

where  $n_b$  is the average background count per packet. In fact, the assumption of complete correlation between the quantum and the probe signal, is not strictly verified in our experiments and eq. (3) turns out to be an approximation of the experimental values. Still, it allows to derive an effective post-selection threshold, as will be seen in the following (e.g., in figure 4).

We now define a further predictive model for estimating the bit error rate on the quantum channel as a function of the probe threshold. Let us assume that the average bit error rate on the quantum channel is  $m_Q$  and that the number of counts per packet due to background noise is  $n_b$ . Now, since background counts output a random result, the corresponding bit error rate is  $1/2$ , and we can write the predicted quantum bit error rate  $Q_{th}$  as a function of the threshold  $V_T$ , namely,

$$Q_{th}(V_T) = m_Q \left( 1 - \frac{n_b}{\bar{S}(V_T)} \right) + \frac{1}{2} \frac{n_b}{\bar{S}(V_T)} \quad (4)$$

where the predicted value for  $\bar{S}(V_T) = \frac{S(V_T)}{N_P(V_T)}$  is obtained by using equation (3). Given these

quantities, the asymptotic key rate of a QKD system based on the BB84 protocol[15] and with the described probe thresholding mechanism reads as follows:

$$R(V_T) = \frac{S(V_T)}{S(0)} [1 - 2h_2(Q(V_T))] \quad (5)$$

It is worth noting that to take into account the asymptotic rate instead of the finite-length one [16, 17], may be considered a restrictive approach, especially because the post-selection further reduces the number of available sifted bits. However, it is sufficient to choose the size of the blocks to be fed as input to the key distillation procedure (i.e., information reconciliation and privacy amplification) such that, without loss of generality, the asymptotic bound provides a reasonable approximation of the actual rate.

In figure 4, we finally compare the theoretical (solid blue line) and the experimental values (blue crosses) for the measured QBER and the asymptotic key rate as a function of the probe intensity threshold in a data acquisition. The curves for the theoretical QBER and for the key rate were obtained by substituting maximum likelihood estimates for the log-normal parameters  $m_V$  and  $\sigma^2$  in eq. (4) and in eq. (5). The other two parameters,  $S(0)$  and  $N_P(0)$ , needed for predicting  $S(T)$  and  $N_P(T)$ , are directly measured (they correspond to the total sifted bits and the total number of packets received respectively).

The experimental data refer to an acquisition of  $5 \cdot 10^5$  sifted bits in condition of high background, simulated by a thermal light source turned on in the receiver laboratory. The intensity of the background was chosen in order to obtain a mean QBER larger than 11%. In particular, we measured an average value of  $n_b = 35.17$  for the background clicks per packet and we assume  $m_Q = 5.6 \cdot 10^{-2}$ . As clearly shown in the figure, eq. (4) provides a good approximation of the experimental curve.

As one can appreciate from the same Figure, we have a remarkable correspondence between the shape of the theoretical rate,  $R_{th}$ , and the measured rate,  $R_{exp}$ . The fact that the experimental points do not fit the expected curve can be ascribed to the discrepancy in the empirical joint distribution of probe intensities and counts with respect to the model; in particular, we measured the following fitting parameters for the normalized log-normal distributions:  $\sigma_V^2 = 0.967$  for the probe intensities and  $\sigma_S^2 = 0.716$ . However, the derivation of the optimal threshold for maximizing the secret key length (magenta dashed line) from the probe distribution yields the optimal  $V_T$  also for the experimental data. In particular, the optimal threshold inferred from the probe distribution is  $V_{T,opt}^{(th)} = 375$  mV, and coincide with the one resulting from optimization on the experimental data, yielding a rate of  $R(V_{T,opt}^{(th)}) = 5.55 \cdot 10^{-2}$ .



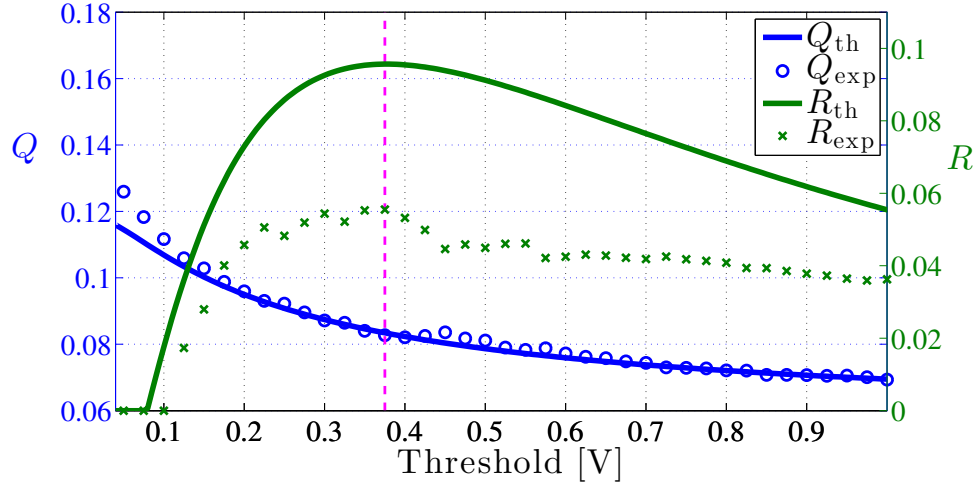


FIG. 4. Experimental QBER ( $Q_{\text{exp}}$ ) and secure key rate ( $R_{\text{exp}}$ ) in function of the probe threshold (measured by the photodiode voltage). With solid lines with show the corresponding theoretical predictions ( $Q_{\text{th}}$  and  $R_{\text{th}}$ ).

Also, we observe that for  $V_T < 70$  mV no key can be extracted, being the QBER higher than the theoretical maximum (i.e.,  $Q = 11\%$ ), whereas by increasing the threshold value a non-zero secret key rate is achievable. With the optimal threshold value, the measured QBER is  $Q(V_{T,\text{opt}}^{(\text{th})}) = 8.38 \cdot 10^{-2}$ ; a significant gain with respect to the initial value,  $Q(0) = 13.14 \cdot 10^{-2}$  is therefore achieved. Finally, we observe that for increasing values of  $V_T > V_{T,\text{opt}}^{(\text{th})}$  the QBER still decreases, but so does the rate, since the reduction in the residual number of sifted bits does not compensate the advantage obtained from the lower QBER. This result is of absolute practical relevance, as it shows that leveraging the probe intensity information is an enabling factor for quantum key distribution, since it allows to distill a secret key even when without the post-selection it would not be possible.

As for the security of this post-selection approach as applied to a QKD system, no advantage is delivered to a potential attacker in the true single photon regime, being the thresholding nothing but a further sifting step on the received bits [10, 12]. If the attacker tried to force Alice and Bob to post-select a particular bit, in fact, she would alter the probe signal *before* the disclosure of the preparation bases on the public channel, and, therefore, before she could actually know if her measured bit is correct. On the other hand, altering the probe statistics or interrupting the probe transmission would not yield any advantage to the attacker, as it would just break the correlation between the quantum and the classical signal and would thus result in a denial of service attack. The security analysis gets more involved if we allow *photon number splitting* (PNS) attacks. In

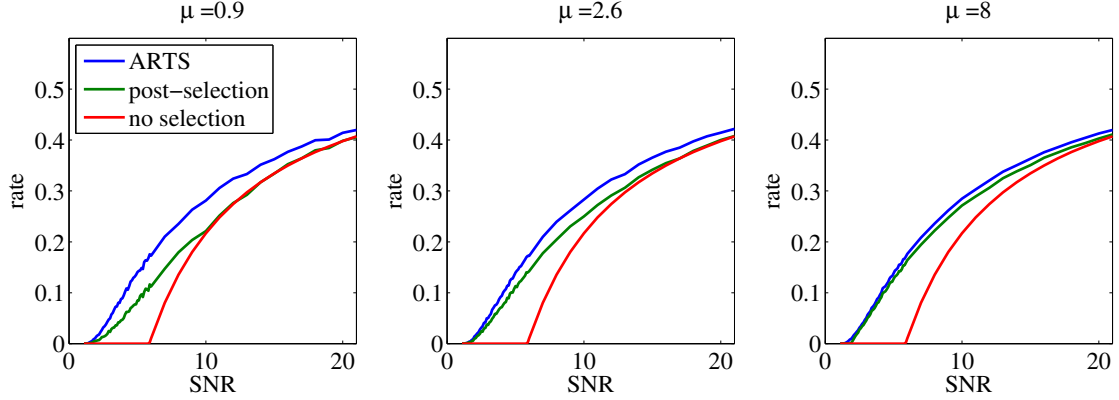


FIG. 5. Comparison between the rates achievable by the ARTS, the post-selection and the standard QKD technique (no selection). We assumed that the channel QBER is 3% and the lognormal parameter is  $\sigma = 1$ , similar to the parameter we measured in the tested free-space channel (see Appendix). The parameter  $\mu$  is the mean sifted bits per coherence time of the channel.

that case, the attacker may force Bob to receive just the qubits for which the PNS attack was successful, i.e., only those pulses with multiple photons. A decoy state protocol may counteract this strategy, but its effectiveness with a turbulent free-space link has to be investigated.

The ARTS can be compared with the technique introduced in [13], where a post-selection is performed when the number of received sifted bits is above a given threshold, determined by the mean QBER of the channel. The post-selection is effective only when the threshold is set in order to get at least several bits for coherence time of the channel (typically of the order of few milliseconds): in fact, only in this condition it is possible to post-select the correct instants of high transmissivity. In the case of very turbulent channel and extreme environmental conditions (say mist or high humidity), the number of received bits per coherence time of the channel can be lower (or of the order) than 10: in this case, the post-selection cannot be implemented and only the ARTS method becomes effective.

We performed a simulation to compare the two techniques by assuming that the probe and the signal statistic are perfectly correlated. The rate achievable in the two cases are shown in figure 5, demonstrating that the ARTS methods outperform the post-selection on the received sifted bits when the number of mean sifted bits received per coherence time of the channel are below  $\sim 10$  and the SNR is below 20.

#### IV. CONCLUSIONS

We have presented a proof of principle demonstration of a method exploiting the atmospheric turbulence as a resource for QKD. The turbulence will implies a fluctuating transmissivity of the channel used for quantum communication. The ARTS method, easily integrable in current QKD systems, is based on the sampling of a classical beam (probe signal) sent on the same channel of the quantum bits. By measuring the intensity of the probe at the receiver, it is possible to select in real time the best time slots of high channel transmissivity. We demonstrated that with the ARTS method we were able to decrease the measured QBER; moreover, this method allows to extract secret key in extreme conditions, namely when the initial average QBER is above the security threshold of 11%.

#### ACKNOWLEDGMENTS

The authors wish to warmly thank for the help provided by Z. Sodnik of the European Space Agency and by S. Ortolani of University of Padova as well as by the Instituto de Astrofísica de Canarias (IAC), and in particular F. Sanchez-Martinez, A. Alonso, C. Warden and J.-C. Perez Arencibia, and by the Isaac Newton Group of Telescopes (ING), and in particular M. Balcells, C. Benn, J. Rey, A. Chopping, and M. Abreu.

This work has been carried out within the Strategic-Research-Project QUINTET of the Department of Information Engineering, University of Padova and the Strategic-Research-Project QuantumFuture (STPD08ZXSJ) of the University of Padova.

#### Appendix A: Experimental setup

The transmitter (Alice) was located at the JKT observatory in the island of La Palma where two 850 nm attenuated lasers provided the quantum signal and a 808 nm laser was used as atmospheric probe. The polarization of the 850 nm lasers was set to the two different bases by means of half wave plates and quarter wave plates. The encoding of the quantum signal was then obtained by controlling the lasers with an FPGA. Classical and quantum lasers were coupled into mode fibers and injected into a fiber beam splitter. One of the two beam splitter output was delivered toward to a suitably designed Galilean telescope whose main characteristic is a singlet aspheric lens of 230 mm diameter and 2200 mm of focal length. This lens allowed us to get, after 143 km of propagation, a beam spot comparable to the dimensions of the primary mirror of the receiving

telescope in order to maximize the power transfer between the two parties. To compensate the beam wandering induced by the atmosphere, we implemented a feedback loop for controlling the transmitting direction: the fiber delivering the signal to the transmitter was mounted on a XYZ movable stage placed close to the focal place of the 230mm lens, with computer controlled stepped motors. On this same stage, we mounted a CCD sensor which acquired a green (532 nm) beacon laser sent by Tenerife toward Alice telescope. The camera is placed in order to measure an image of the singlet focal plane: the wandering of the beacon on the CCD was then analyzed in real time by a software that moves the XYZ stage to compensate the movement of the beacon spot on the camera.

At the receiver part (Bob), in Tenerife, we used the 1 m aperture telescope of the ESA Optical Ground Station to receive the signals. After the Coud path, we collimated the beam and the classical and quantum signal (at different wavelength) were divided by a dichroic mirror. The qubits were measured in two bases, using PBS and waveplates. The counts detected by the two single-photon avalanche photodiodes (SPAD) were stored on a FPGA. The probe beam is detected by an high-bandwidth APD (avalanche photodetector) and then registered and stored by an oscilloscope.

For what concerns the transmitted qubits, in order to measure the QBER of the channel, we used the same data structure of a recent free-space QKD implementation based on the B92 protocol [18, 19]. A raw key is composed into  $N$  packets of 2880 bits each, sent at the rate of 2.5 Mhz; as regards the payload slots, Alice sends two qubits separated by 200 ns. Due to communication with the FPGA, each packets is sent every 20ms resulting in an average sending rate of 150kHz. The two FPGAs are synchronized every second by a pulse-per-second (pps) signal equipped by two GPS receivers located in the two islands.

We want to point out that at the transmitter side, the pulses contain in average more than one photon, while at the receiver side we work in the single photon regime. Our aim, in fact, was to simulate a possible realistic scenario where one would employ fast (hundreds of MHz to GHz) free-space QKD systems which are nowadays commonly available. Since our system has a transmission rate of 2.5 MHz, the detected rate is comparable to the rate observable with a transmitter emitting true single photon pulses with a repetition rate of about 1GHz, considering fixed the amount of optical and atmospheric attenuation.

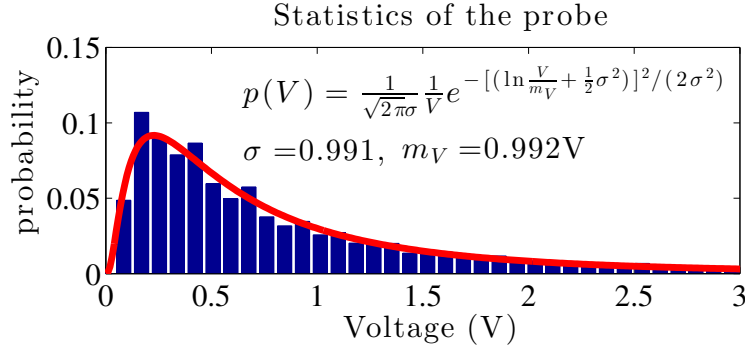


FIG. 6. Experimental occurrences of probe intensities (measured by photodiode voltages) and lognormal fit.

### Appendix B: Log-normal distribution

Here we show the distribution of the measured voltages of the data used in Figure 2. According to the theory [9, 14], they follow a log-normal distribution. In Figure 6 we show the experimental probabilities of occurrence of different photodiode voltages corresponding to different probe intensities. We also show the corresponding lognormal curve that fits the experimental data. In the figure we report the lognormal parameters obtained in the fit.

- 
- [1] Europe: <http://qurope.eu/content/Roadmap> and in particular <http://qurope.eu/content/416-towards-long-distances-satellite-quantum-communication>; Japan: <http://qict.nict.go.jp/about/50roadmap.html>; USA [http://qist.lanl.gov/qcrypt\\_map.shtml](http://qist.lanl.gov/qcrypt_map.shtml) and in partic .
  - [2] B. C. Jacobs and J. D. Franson, *Optics Letters* **21**, 1854 (1996).
  - [3] W. Buttler, *et al.*, *Physical Review Letters* **81**, 3283 (1998).
  - [4] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, *New J. Phys.* **4**, 43 (2002).
  - [5] J. E. Nordholt, R. J. Hughes, G. L. Morgan, C. G. Peterson, and C. C. Wipf, in G. S. Mecherle, editor, *Proc. SPIE 4635*, 116–126 (2002).
  - [6] D. Elser, T. Bartley, B. Heim, C. Wittmann, D. Sych, and G. Leuchs, *New Journal of Physics* **11**, 045014 (2009).
  - [7] M. Peev, *et al.*, *New Journal of Physics* **11**, 075001 (2009).
  - [8] M. García-Martínez, N. Denisenko, D. Soto, D. Arroyo, A. B. Orue, and V. Fernandez, *Applied Optics* **52**, 3311 (2013).
  - [9] I. Capraro, A. Tomaello, A. Dall’Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, *Phys. Rev. Lett.* **109**, 200502 (2012).
  - [10] J. Bae and A. Acín, *Physical Review A* **75**, 012334 (2007), 0610048.

- [11] U. Maurer, IEEE Transactions on Information Theory **39**, 733 (1993).
- [12] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, Physical Review A **76**, 032312 (2007).
- [13] C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, New Journal of Physics **14**, 123018 (2012).
- [14] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, Journal of Optics B: Quantum and Semiclassical Optics **6**, S742 (2004).
- [15] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 175, IEEE, New York (1984).
- [16] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, Nature Communications **4**, 2363 (2013).
- [17] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).
- [18] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
- [19] M. Canale, D. Bacco, S. Calimani, F. Renna, N. Laurenti, G. Vallone, and P. Villoresi, in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies - ISABEL '11*, 1–5, ACM Press, New York, NY, USA (2011), ISBN 9781450309134.